EP 1360(3)

A1

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32 — A1

(11) International Publication Number: **WO 98/37663**

(43) International Publication Date: 27 August 1998 (27.08.98)

(21) International Application Number: PCT/SE98/00206

(22) International Filing Date: 5 February 1998 (05.02.98)

(30) Priority Data:
9700587-0 19 February 1997 (19.02.97) SE

(71) Applicant *(for all designated States except US)*: POSTGIROT BANK AB (publ) [SE/SE]; S-105 06 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: LEONARDI, Robert [SE/SE]; Gränsvägen 350, S-163 52 Spånga (SE).

(74) Agents: ÖRTENBLAD, Bertil et al.; Noréns Patentbyrå AB, P.O. Box 10198, S-100 55 Stockholm (SE).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR AUTHORIZATION CHECK

(57) Abstract

Method for checking authorization incorporating a way to impart to a so-called smart card (SmartCard) an encryption key or equivalent key and including a way to cause a microprocessor, by means of the encryption key and at least one number, to perform a calculation whose result comprises a signature, and including a way to have said signature together with said number transferred to a system for which authorization is to be shown which includes a computer in which said encryption key is stored, said computer being programmed to carry out said calculation to obtain said signature and then to compare the latter signature with the first-mentioned signature.

Method for authorization check

The present invention relates to a method for checking the authorization of a person, in his/her capacity as user of a system such as a payment system or a data system.

Systems now in existence are used to check the authorization of a person in connection with payment. One such system is used within the Swedish Postal Service for payments made via postgiro. In accordance with this system, the customer receives a so-called SmartCard and a card reader for it. An encryption key is stored on the SmartCard, and it can be read by a microprocessor on the SmartCard after a PIN code has been entered.

The said encryption key is stored not only on the SmartCard, but also at the Swedish Postal Service postgiro department where it is linked to a specific person.

When a payment is to be made, the user keys in the said PIN code, the number of the account to which the payment is to be sent and the amount in question. Herewith, the microprocessor performs a calculation based on the amount, the account number and the encryption key in accordance with the so-called DES (Data Encryption Standard) algorithm, wherewith a signature is generated by the said calculation. After this is done, the amount, the account number and the signature are transferred to the postgiro department in a suitable manner, via data, mail or fax for example.

The postgiro department receives the information and then performs the same calculation as set forth above and compares the result with the signature that was transferred. If the comparison results in a match, an authorized person, i.e. the holder of the SmartCard, is deemed to have ordered the transaction, wherewith the transaction is executed. The transaction is executed by transferring money from the postgiro

ture, characterized in that the said smart card is a so-called SIM-card intended for mobile telephony and a memory in said SIM-card is, in a first step, provided with unique information containing a unique identity in order to communicate telephonically using a mobile telephone and in that, in a second step, the SIM-card memory is provided with said encryption key, and in that a system for which authorization is to be shown is provided with the same encryption key linked to an identity of the SIM-card, and in that in response to the entry of an appropriate code and at least the said number via the keyboard on the mobile telephone, a microprocessor on the said SIM-card is induced to perform the said calculation resulting in the said signature.

The present invention is not limited to any special field with regard to showing authorization. Instead, it is applicable for all kinds of systems such as payment systems, data systems, systems that check authorization before allowing entrance etc.

The description of the present invention that follows, however, is for a system that provides payment via postgiro.

The system is described in greater detail below, partially in connection with an example of an embodiment shown on the attached drawing, where:

- Fig. 1 shows the included hardware schematically.
- Fig. 2 shows a SIM-card.
- Fig. 3 shows a schematic view of a block diagram for which a function is described.
- Fig. 4 shows a schematic view of a block diagram for which another function is described.

Fig. 1 shows mobile telephone 1 of an appropriately known type which is intended for use in a GSM system or an equivalent telephone system where a so-called smart card

memory 7 in said SIM-card 6 in such a way as to support telephonic communication using a mobile telephone. This appropriately takes place in the same as way as presently being used in the GSM system.

In a second step, the memory in SIM-card 6 is provided with the said encryption key. This memory can be the existing memory 7 or an extra memory. This is accomplished in a way that corresponds with the way the previously mentioned identity was entered, but it should preferably be carried out by the person who controls the system for which authorization is to be shown.

In accordance with the invention, the system for which authorization is to be shown is provided with the same encryption key linked to an identity for the SIM-card. Here, for example, the IMSI used for the SIM-card can serve as its identity ID. Alternatively, the encryption key in the said system can be linked to some other identity such as the user's telephone number, a customer number or a name. What is essential is that the system must later be able to retrieve the correct encryption key for a specified user.

The invention is further characterized in that when a suitable code is entered along with at least the said number via keyboard 2 on mobile telephone 1, a microprocessor on the said SIM-card is induced to perform the said calculation resulting in the said signature. The microprocessor can be the regular microprocessor that is normally incorporated into the SIM-card, but it can also be a separate microprocessor on the SIM-card. In the latter case, however, the separate microprocessor is linked to regular microprocessor 7 on the SIM-card.

The term "suitable code" means, for example, a code that is entered in order to put the mobile telephone in a mode in

In accordance with an alternative embodiment, the signature calculated by the mobile telephone together with at least the said numbers is caused to be transferred directly from the mobile telephone to said system via an interface between the mobile telephone and the system such as a computer 5 belonging to the system. The interface can comprise a cable 8 or an infrared link or some other suitable link.

In accordance with a preferred embodiment, the mobile telephone is caused to present the said signature on the mobile telephone display. In such case, the user can, for example, enter the said numbers and signature on a keyboard belonging to a computer that belongs to the system.

In accordance with a highly preferred embodiment, a special PIN code is assigned to the SIM-card in such a way that it can be used to enable the card for said calculation of the signature. This further enhances security since the user must a) know his/her PIN code to start the mobile telephone and b) know his/her PIN code to access and start the calculation process used to obtain the electronic signature.

To facilitate the making of correct payments for example and in accordance with a preferred embodiment, the mobile telephone is caused to present the said numbers on its display. An account number and an amount, for example, can be displayed before the signature is calculated.

When the signature has been calculated, data is thus transferred to the system. Herewith, as illustrated in Fig. 4, a user identity ID such as a telephone number, an IMSI or some other identity is always transferred. Signature SIG is also always transferred. Moreover, at least one number D1 or D2 is always transferred. If payments are involved, account number D1 and amount D2 are transferred. When this has happened, the system computer 5 retrieves the encryption key KEY that is linked to identity ID from a memory MEM and then calculates

Claims

1. Method for checking authorization incorporating a way to impart to a so-called smart card (SmartCard) an encryption key or equivalent key and a way to induce a microprocessor, by means of the encryption key and at least one number, to carry out a calculation whose result comprises a signature, and a way to have said signature, together with said number, transferred to a system for which authorization is to be shown, where said system includes a computer in which said encryption key has been stored and to have said system perform said calculation whose result will comprise said signature, and a way to have the computer compare the latter signature with the first-mentioned signature characterized in that said smart card is a so-called SIM-card (6) intended for mobile telephony, and in that the memory (MEM) on said SIM-card is, in a first step, provided with unique information including a unique identity in order to communicate telephonically using a mobile telephone, and in that the memory on the SIM-card in a second step is provided with said encryption key (KEY), and in that a system for which authorization is to be shown is provided with the same encryption key (KEY) linked to an identity of SIM-card (6), and in that when a suitable code (PIN) is entered along with at least said number via the keyboard (2) on the mobile telephone (1), a microprocessor (7) on the said SIM-card is induced to perform the said calculation resulting in the said signature (SIG).

2. A method in accordance with claim 1, characterized in that the said number contains at least two numbers.

3. A method in accordance with claim 1 or 2, characterized in that the signature (SIG) calculated by the mobile telephone (1, 7) together with at least the said number is caused to be transferred to said system (5) via the mobile telephone network.

Fig. 1

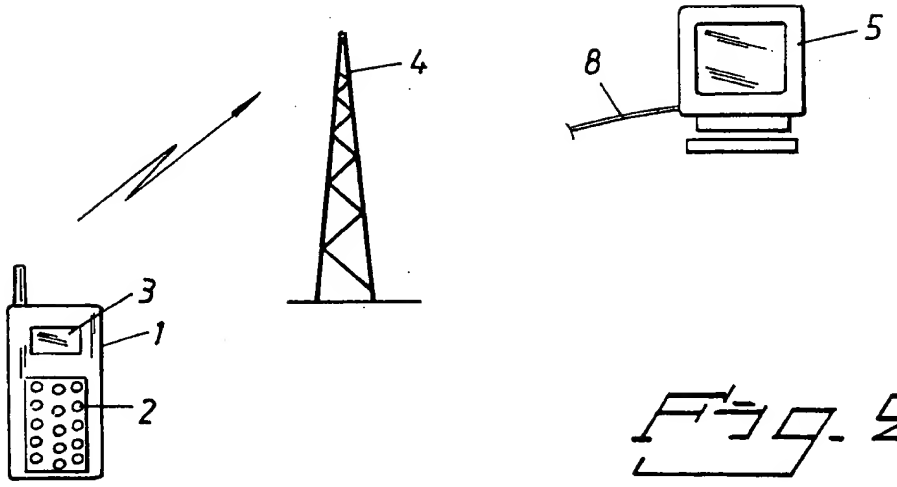


Fig. 2

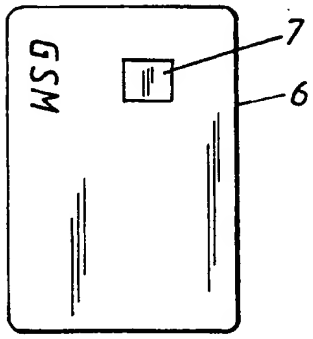


Fig. 3

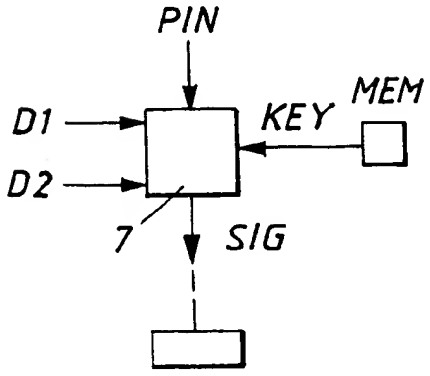
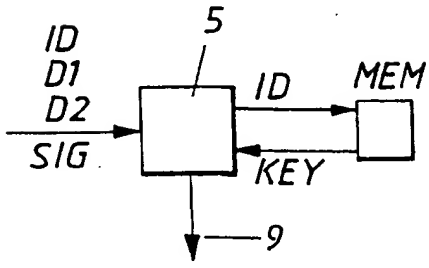


Fig. 4



INTERNATIONAL SEARCH REPORT

Information on patent family members

30/06/98

International application No.
PCT/SE 98/00206

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9605702 A2	22/02/96	BR 9506293 A	11/11/97
		CA 2171017 A	22/02/96
		EP 0721718 A	17/07/96
		FI 961404 A	28/03/96
		JP 9503895 T	15/04/97
		US 5537474 A	16/07/96
		US 5668875 A	16/09/97
EP 0708547 A2	24/04/96	CA 2156206 A	23/03/96
		JP 8096043 A	12/04/96
		US 5608778 A	04/03/97
WO 9613814 A1	09/05/96	EP 0739526 A	30/10/96
		FI 100137 B	00/00/00
		FI 945075 A	29/04/96
		FI 962553 A	25/11/97
		FI 962961 A	28/08/96
		FI 971009 A	26/04/97
		FI 971248 A	26/04/97
		FI 971848 A	30/04/97
WO 9411849 A1	26/05/94	AT 159602 T	15/11/97
		DE 69314804 D,T	12/02/98
		EP 0669031 A,B	30/08/95
		SE 0669031 T3	
		ES 2107689 T	01/12/97
		FI 925135 A	12/05/94
		FI 934995 A	12/05/94
		NO 951814 A	09/05/95

European Patent Office

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 00 96 1057

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X ✓	GB 2 261 538 A (THE GOVERNOR AND COMPANY OF THE BANK OF SCOTLAND) 19 May 1993 (1993-05-19)	1,2	G06F17/60
A	* the whole document *	4-12, 16-28	
A ✓	US 4 910 774 A (S. BARAKAT) 20 March 1990 (1990-03-20) * abstract; claims; figures * * column 4, line 38 - column 6, line 24 *	1,3-10, 18-20, 25-29	
A ✓	WO 98/37663 A (POSTGIROT BANK) 27 August 1998 (1998-08-27) * the whole document *	1-35	
A ✓	US 5 396 558 A (G. ISHIGURO ET AL.) 7 March 1995 (1995-03-07) * abstract; claims; figures * * column 6, line 26 - column 9, line 30 *	1-35	
A ✓	US 5 731 576 A (J-L. VALADIER) 24 March 1998 (1998-03-24) * abstract; claims; figures *	1-35	TECHNICAL FIELDS SEARCHED (IPC) G07G G07F
A ✓	US 4 825 052 A (F. CHEMIN ET AL.) 25 April 1989 (1989-04-25) * abstract; claims; figures * * column 5, line 25 - column 7, line 59 *	1-29	
A ✓	EP 0 316 689 A (TOSHIBA) 24 May 1989 (1989-05-24)		
A ✓	US 5 440 634 A (T.L. JONES ET AL.) 8 August 1995 (1995-08-08)		
A ✓	FR 2 710 769 A (INNOVATRON SECURITE INFORMATIQUE) 7 April 1995 (1995-04-07)		

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
The Hague	12 January 2006	David, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 96 1057

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-01-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2261538 A	19-05-1993	NONE	
US 4910774 A	20-03-1990	EP 0299826 A1	18-01-1989
		FR 2618002 A1	13-01-1989
		JP 1093858 A	12-04-1989
WO 9837663 A	27-08-1998	AU 725952 B2	26-10-2000
		AU 6126898 A	09-09-1998
		BR 9807372 A	14-03-2000
		CA 2281816 A1	27-08-1998
		CN 1248367 A	22-03-2000
		EP 0962071 A1	08-12-1999
		JP 2001513274 T	28-08-2001
		NO 993939 A	19-10-1999
		SE 508844 C2	09-11-1998
		SE 9700587 A	20-08-1998
		US 6556680 B1	29-04-2003
US 5396558 A	07-03-1995	DE 69322463 D1	21-01-1999
		DE 69322463 T2	10-06-1999
		DE 69332745 D1	10-04-2003
		DE 69332745 T2	16-10-2003
		EP 0588339 A2	23-03-1994
US 5731576 A	24-03-1998	AT 156922 T	15-08-1997
		DE 69500561 D1	18-09-1997
		DE 69500561 T2	11-12-1997
		EP 0744063 A1	27-11-1996
		ES 2105892 T3	16-10-1997
		FR 2716021 A1	11-08-1995
		WO 9522125 A1	17-08-1995
US 4825052 A	25-04-1989	DE 3669216 D1	05-04-1990
		EP 0231702 A1	12-08-1987
		FR 2592510 A1	03-07-1987
		JP 1919714 C	07-04-1995
		JP 6044267 B	08-06-1994
		JP 62222360 A	30-09-1987
EP 0316689 A	24-05-1989	DE 3850553 D1	11-08-1994
		DE 3850553 T2	27-10-1994
		JP 1129379 A	22-05-1989
		JP 2698588 B2	19-01-1998
		KR 9107758 B1	30-09-1991
		US 5017766 A	21-05-1991

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 96 1057

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-01-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5440634 A	08-08-1995	AT 145744 T	15-12-1996
		AU 663739 B2	19-10-1995
		AU 2888692 A	21-05-1993
		BR 9205416 A	17-05-1994
		CA 2098481 A1	17-04-1993
		DE 69215501 D1	09-01-1997
		DE 69215501 T2	27-03-1997
		DK 567610 T3	17-02-1997
		EP 0567610 A1	03-11-1993
		ES 2096772 T3	16-03-1997
		WO 9308545 A1	29-04-1993
		GR 3022528 T3	31-05-1997
		HK 1001573 A1	26-06-1998
		JP 2853331 B2	03-02-1999
		JP 6503913 T	28-04-1994
		KR 161670 B1	20-03-1999
		MD 1402 F2	31-01-2000
		NO 932217 A	12-08-1993
		PL 299825 A1	18-04-1994
		RU 2137187 C1	10-09-1999
FR 2710769 A	07-04-1995	NONE	